IN THE CLAIMS:

1-39 (cancelled).

40 (new). A method for performing a cryptographic operation that comprises transforming digital information, the method comprising:

providing digital information;

providing a digital operator having a component selected from a large set of elements;

expanding the component into a plurality of factors, each factor having a low hamming weight; and

transforming the digital information using the digital operator, said transforming comprising computing multiples;

said method further comprising:

selecting a ring R;

selecting an R-module M;

selecting two or more subsets R_1, R_2, ..., R_k of R with the property that r_1 is an element in R_1, r_2 is an element in R_2,...and r_k is an element in R_k;

computing $r * m$, where r is in R and m is in M, by expanding r as $r_1 * r_2 * \ldots r_k$, where k is an integer and computing the quantity $r_1 * (r_2 * (\ldots (r_k * m)$.

41 (new). The method of claim 40, wherein the cryptographic operation is selected from a group consisting of key generation, encryption, decryption, creation of a

digital signature, verification of a digital signature, creation of a digital certificate, authentication of a digital certificate, identification, pseudorandom number generation and computation of a hash function.

42 (new). The method of claim 40, wherein each r_k has a Hamming weight that is less than about 15.

43 (new). The method of claim 40, wherein each r_k has a Hamming weight that is less than about 10.

44 (new). The method of claim 40, wherein the subset R_i is a subset of R consisting of elements of the form.

$$a_1 t^{e(1)} + a_2 t^{e(2)} + \ldots + a_n t^{e(n)},$$

where n is an integer.

45 (new). The method of claim 44, wherein each of the elements $a_1, \ldots, a_n$ are chosen from the set {0,1}.

46 (new). The method of claim 44, wherein each of the elements $a_1, \ldots, a_n$ are chosen from the set {-1,0,1}.

47 (new). The method of claim 40, wherein the subset R_i is a subset of R

consisting of polynomials in elements of $t_1, \ldots, t_k$ of R having coefficients $a_1, \ldots, a_k$ taken from a subset A of R where k is an integer.

48 (new). The method of claim 47, wherein each of the coefficients $a_1, \ldots, a_k$ is chosen from the set {0,1}.

49 (new). The method of claim 47, wherein each of the coefficients $a_1, \ldots, a_k$ is chosen from the set {-1,0,1}.

50 (new). The method of claim 40, wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets $R_1, \ldots, R_k$ consist of integers of the form

$$a_1 p^{e(1)} + a_2 p^{e(2)} + \ldots + a_n p^{e(n)},$$

wherein n is an integer that is less than m and wherein $a_1, \ldots, a_n$ are elements of the set {0,1}.

51 (new). The method of claim 40, wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets $R_1, \ldots, R_k$ consist of integers of the form

$$a_1 p^{e(1)} + a_2 p^{e(2)} + \ldots + a_n p^{e(n)},$$

wherein n is an integer that is less than m and wherein $a_1, \ldots, a_n$ are elements of a small set of integers A.

52 (new). The method of claim 40, wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q).

53 (new). The method of claim 40, wherein the module M is a group of points e(GF(q)) of an elliptic curve E over a finite field GF(q).

54 (new). The method of claim 44, wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p, wherein the module M is a group of points E(GF(q)) and wherein the element t is a p-power Frobenius map.

55. (new). The method of claim 44, wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p, wherein the module M is a group of points E(GF(q)) and wherein the element t is a point halving map.

56 (new). The method of claim 40, wherein the ring R is a ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the subsets $R_1,\ldots, R_k$ are sets of polynomials with few nonzero terms.

57 (new). The method of claim 56, wherein the ideal I is the ideal generated by the polynomimial X^N-1.

58 (new). The method of claim 56, wherein the ring R is a finite ring **Z/qZ** of integers modulo q, wherein q is a positive integer.

59 (new). The method of claim 44, wherein the ring R is a ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the element t is the polynomial X in R.

60 (new). The method of claim 59, wherein the deal I is the ideal generated by the polynomimial X^N-1.

61 (new). The method of claim 59, wherein the ring R is a finite ring Z/qZ of integers modulo q, wherein q is a positive integer.

62 (new). A computer readable medium containing instructions for a method for performing a cryptographic operation that comprises transforming digital information, the method comprising:

providing digital information;

providing a digital operator having a component selected from a large set of elements;

expanding the component into a plurality of factors, each factor having a low hamming weight; and

transforming the digital information using the digital operator, said

transforming comprising computing multiples;

said method further comprising:

selecting a ring R;

selecting an R-module M;

selecting two or more subsets R_1, R_2, ..., R_k of R with the property that r_1 is an element in R_1, r_2 is an element in R_2,...and r_k is an element in R_k;

computing $r * m$, where r is in R and m is in M, by expanding r as $r_1 * r_2 * \ldots r_k$, where k is an integer and computing the quantity $r_1 * (r_2 * (\ldots(r_k * m)$.

63 (new). The computer readable medium of claim 62, containing instructions for a method wherein the subset R_i is a subset of R consisting of elements of the form.

$$a_1 t^{e(1)} + a_2 t^{e(2)} + \ldots + a_n t^{e(n)},$$

where n is an integer.

64 (new). The computer readable medium of claim 62, containing instructions for a method wherein the subset R_i is a subset of R consisting of polynomials in elements of t_1, ..., t_k of R having coefficients a_1, ..., a_k taken from a subset A of R where k is an integer.

65 (new). The computer readable medium of claim 62, containing instructions for a method wherein the ring R is the ring of integers, the R-module M is a group of

nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets $R_1, \ldots,$ R_k consist of integers of the form

$$a_1p^{e(1)} + a_2p^{e(2)} + \ldots + a_np^{e(n)},$$

wherein n is an integer that is less than m and wherein $a_1, \ldots, a_n$ are elements of the set $\{0,1\}$.

66 (new). The computer readable medium of claim 62, containing instructions for a method wherein the ring R is the ring of integers, the R-module M is a group of nonzero elements in the field $GF(p^m)$ with p^m elements, and wherein the subsets $R_1, \ldots,$ R_k consist of integers of the form

$$a_1p^{e(1)} + a_2p^{e(2)} + \ldots + a_np^{e(n)},$$

wherein n is an integer that is less than m and wherein $a_1, \ldots, a_n$ are elements of a small set of integers A.

67 (new). The computer readable medium of claim 62, containing instructions for a method wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q).

68 (new). The computer readable medium of claim 62, containing instructions for a method wherein the module M is a group of points e(GF(q)) of an elliptic curve E over a finite field GF(q).

69 (new). The computer readable medium of claim 63, containing instructions for a method wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p, wherein the module M is a group of points E(GF(q)) and wherein the element t is a p-power Frobenius map.

70 (new). The computer readable medium of claim 63, containing instructions for a method wherein the ring R is an endomorphism ring of a group of points E(GF(q)) of an elliptic curve E over a finite field GF(q) of characteristic p, wherein the module M is a group of points E(GF(q)) and wherein the element t is a point halving map.

71 (new). The computer readable medium of claim 62, containing instructions for a method wherein the ring R is a ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the subsets $R_1, \ldots, R_k$ are sets of polynomials with few nonzero terms.

72 (new). The computer readable medium of claim 63, containing instructions for a method wherein the ring R is a ring of polynomials modulo an ideal A[X]/I, wherein A is a ring and I is an ideal of A[X], and wherein the element t is the polynomial X in R.